PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215279
(43)Date of publication of application : 04.08.2000

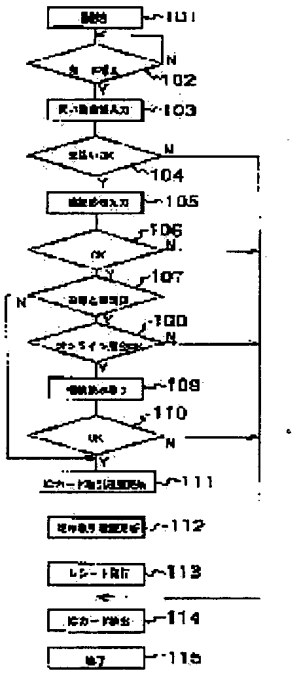
(51)Int.Cl. G06K 17/00
G07D 9/00
G07F 7/12
G07F 7/08

(21)Application number : 11-017174
(22)Date of filing : 26.01.1999

(71)Applicant : HITACHI LTD
HITACHI VIDEO & INF SYST INC
(72)Inventor : MATSUMOTO KENJI
ITO SHIGEYUKI
TAKAMI MINORU
INOUE MASAYUKI
YONEDA KOICHI
INAMITSU TETSUJI
YAMAUCHI TSUKASA
INOUE YOSHITAKE

(54) IC CARD SETTLEMENT DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To dynamically optimize the relation between the cost required for identity certification and the certainty of identity certification in accordance with a value which is to be protected by identity certification.
SOLUTION: The input of a shopping amount and a password is received (steps 103 and 105). When the shopping amount is lower than a setting value (Step 107), settlement is executed (steps 111 and 112) if the inputted password matches with a password stored in an IC card. When the shopping amount is higher than the setting value (step 107), the fingerprint of a user is read (step 109) and settlement is executed (steps 111 and 112) only when the fingerprint which is read matches with a fingerprint stored in the IC card (S110).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－215279
（P2000－215279A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｌ	３Ｅ０４０
			Ｓ	３Ｅ０４４
			Ｖ	５Ｂ０５８
Ｇ０７Ｄ　9/00	４３６	Ｇ０７Ｄ　9/00	４３６Ｚ	
	４６１		４６１Ａ	

審査請求　未請求　請求項の数12　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願平11－17174

(22)出願日　平成11年１月26日(1999.1.26)

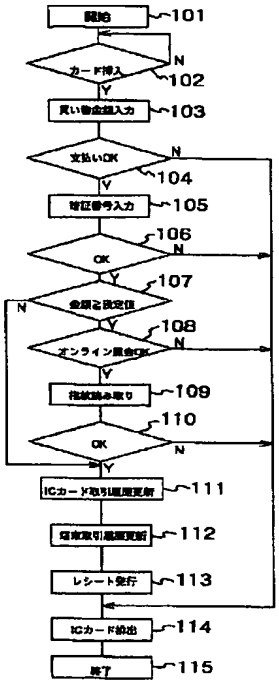
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000233136
株式会社日立画像情報システム
神奈川県横浜市戸塚区吉田町292番地
(72)発明者　松本　健司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内
(74)代理人　100087170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　ＩＣカード決済装置

(57)【要約】
【課題】本人認証に要するコストと本人認証の確度との関係を本人認証によって守るべき価値に応じて動的に最適化する。
【解決手段】買い物金額と暗証番号の入力を受け付け（ステップ１０３、１０５）、買い物金額が設定値より低額である場合（ステップ１０７）は、入力された暗証番号とICカードに記憶された暗証番号が一致すれば（ステップ１０６）、決済を行う（ステップ１１１、１１２）。一方、買い物金額が設定値より高額である場合（ステップ１０７）は、利用者の指紋を読み取り（ステップ１０９）、読み取った指紋とICカードに記憶された指紋が一致した場合にのみ（ステップ１１０）、決済を行う（ステップ１１１、１１２）。

図3



1

【特許請求の範囲】

【請求項１】ICカードの正当な所有者の暗証番号と生体情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置であって、

決済を行う金額の入力を受け付ける決済額受け付け手段と、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

入力された決済を行う金額が所定値より低額である場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第１決済手段と、

入力された決済を行う金額が所定値より高額である場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第２決済手段とを有することを特徴とするICカード決済装置。

【請求項２】ICカードの正当な所有者の暗証番号と、生体情報と、ICカードを用いた決済の回数を算出可能な当該ICカードを用いた決済の履歴情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置であって、

決済を行う金額の入力を受け付ける決済額受け付け手段と、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

ICカードに記憶された履歴情報から求まる当該ICカードを用いた決済の回数が所定値を超えない場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第１決済手段と、

ICカードに記憶された履歴から求まる当該ICカードを用いた決済の回数が所定値を超える場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第２決済手段と、

決済が行われた場合に、行われた決済の内容に応じてICカードに記憶された履歴情報を更新する履歴情報更新手段とを有することを特徴とするICカード決済装置。

【請求項３】ICカードの正当な所有者の暗証番号と、生体情報と、ICカードを用いた決済の金額の累計を算出可能な当該ICカードを用いた決済の履歴情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置であって、

決済を行う金額の入力を受け付ける決済額受け付け手段と、

2

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

ICカードに記憶された履歴情報から求まる当該ICカードを用いた決済の金額の累計が所定値を超えない場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第１決済手段と、

ICカードに記憶された履歴から求まる当該ICカードを用いた決済の金額の累計が所定値を超える場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第２決済手段と、

決済が行われた場合に、行われた決済の内容に応じてICカードに記憶された履歴情報を更新する履歴情報更新手段とを有することを特徴とするICカード決済装置。

【請求項４】請求項１、２または３記載のICカード決済装置であって、

前記第２決済手段は、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号とが一致し、かつ、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報とが一致した場合にのみ決済を行うことを特徴とするICカード決済装置。

【請求項５】請求項１、２、３または４記載のICカード決済装置であって、

前記第１決済手段は、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号とが一致しない場合には、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行うことを特徴とするICカード決済装置。

【請求項６】ICカードの正当な所有者の暗証番号と生体情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置であって、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、両暗証番号が一致しない場合に、さらに、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う決済手段とを有することを特徴とするICカード決済装置。

【請求項７】請求項１、２、３、４、５または６記載のICカード決済装置であって、

ICカード使用者から、今後使用を希望する新しい暗証番

号の入力を受け付ける新暗証番号受け付け手段と前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合にICカードに記憶された暗証番号を、新暗証番号受け付け手段が受け付けた新しい暗証番号に更新する暗証番号更新手段とを有することを特徴とするICカード決済装置。

【請求項８】請求項１、２、３、４、５、６または７記載のICカード決済装置であって、

前記生体情報は、指紋の情報であることを特徴とするICカード決済装置。

【請求項９】ICカードに記憶された当該ICカードの正当な所有者の暗証番号と指紋情報とを用いて、ICカード使用者の認証を行なうICカード処理装置であって、

ICカード使用者より、指先による暗証番号の入力を受け付ける入力部と、当該入力部に暗証番号入力のために置かれた指先から指紋情報を読み取る読み取り部とを有することを特徴とするICカード処理装置。

【請求項１０】ICカードの所有者の個人情報が記憶されたＩＣカードを処理するICカード処理装置であって、

ICカード使用者に、サービスを提供するためのユーザインタフェースを供する手段と、

ICカードに記憶された個人情報に応じて、ICカード使用者に供するユーザインタフェースをカスタマイズする手段とを有することを特徴とするICカード処理装置。

【請求項１１】ICカードの正当な所有者の暗証番号と生体情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置において、ICカード使用者を認証する方法であって、

ICカードの不正使用による損害の可能額が低額である場合に、ICカード使用者より受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、ICカードの不正使用による損害の可能額が高額である場合に、ICカード使用者より読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第２決済手段とを有することを特徴とするICカード使用者を認証する方法。

【請求項１２】ICカードの正当な所有者の暗証番号と個人情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置において、ICカード使用者を認証する方法であって、

ICカードの不正使用による損害の可能額が低額である場合に、ICカード使用者より受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、ICカードの不正使用による損害の可能額が高額である場合に、ICカード使用者より受け付けた個人情報とICカードに記憶された個人情報との一致を調べ、両個人情報が一致した場合に決済を行う第２決済手段とを有することを特徴とするICカード使用者を認証する方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クレジット情報や電子マネー情報などを格納したＩＣカードを用いた決済を行うＩＣカード決済装置に関するものである。

【０００２】

【従来の技術】現在、取引者間の現金以外の取引の決済の方法としては、クレジットカードによる決済が一般的である。また、クレジットカードとしては、磁気ストライプカードを使用した物が主流であり、その決済の手順は一般的には次のようなものである。

【０００３】すなわち、まず、買い物時に購入者が販売者にクレジットカードを渡す。販売者は、磁気ストライプリーダーを用いて磁気ストライプに格納されているカードのクレジット番号を読み出す。その後、電話回線を使用してクレジットカードの照会センタに接続し、読み取ったクレジット番号をオンラインで照会する。そして、照会の結果、過去に、このクレジットカードによるに不正な買い物が無いことが確認されると、購入者のサインによりカード所有者本人であることを確認し、クレジットによる販売を行い、販売の内容をクレジット会社に通知する。この場合、後日、販売者への支払いはクレジット会社より、購入者の支払いはクレジット会社に対して行われる。

【０００４】このような従来のクレジットカードを利用した決済の方法は、クレジットカードの偽造、盗難、サインの模倣などによるクレジットカードの不正使用が行われることを充分に防止することができなかった。また、前述したオンライン照会によって、クレジットカードの不正使用が繰り返されることを防止する技術も、実際には、少額取引の場合には販売者がオンライン照会を省略してしまうことがあるため、必ずしも常に有効に機能しているとは言えなかった。

【０００５】さて、最近ではＩＣカードを使用した新しい決済方法が、さかんに提案、実験されている。

【０００６】その一つが、クレジットカードを、ＩＣカード化したものであり、他の一つが、ＩＣカードを使用した電子マネーである。ＩＣカード内のメモリに電子マネーを格納し、取引時には、現金の代わりに、ＩＣカード間で電子マネーをやりとりしようとするものである。

【０００７】そして、いずれの場合も、ICカードの不正使用を防ぐためには、ICカード使用者がICカードの正当な所有者であることを確認する本人認証が重要となる。

【０００８】このようなICカード所有者の本人認証を行う技術としては、ICカード内にICカード所有者の暗証番号をICカード外から知ることができないように記録しておき、決済時には、ICカード決済装置にICカードを装着し、ICカードにおいて、ICカード使用者がICカード決済装置に入力した暗証番号と、装着されたICカードに記録

5

された暗証番号とを照合し、一致した場合に、本人と認証しようとするものがある。これは、従来のクレジットカードのサインの代わりに暗証番号を使用しようとするものであり、この技術は、利用者が、取引のたびに、いちいちサインする手間を不要とすることができると共に、暗証番号をICカード外から知ることができないようにICカードに記憶するため、この暗証番号をサインのように、簡単に第三者が知ることができないという点で、従来のクレジットカードより優れている。

【０００９】また、ICカード所有者の本人認証を行う技術としては、ICカード内にICカード所有者の生体情報を記録しておき、決済時には、ICカード決済装置にICカードを装着し、ICカード決済装置において、ICカード使用者からICカード決済装置に生体情報を取り込み、装着されたICカードに記録された生体情報と照合し、一致した場合に、本人と認証しようとするものがある。これは、従来のクレジットカードのサインの代わりに生体情報を使用しようとするものであり、この技術は、利用者が暗証番号を覚える必要がなく、生体情報が、正当なICカード所有者独自かつ不可分のものであることより、より高い精度で本人認証を行えることが期待できる点で、暗証番号を用いる技術より優れている。なお、生体情報の代表的なものとしては、指紋、掌紋、虹彩、網膜などの形状がある。

【００１０】

【発明が解決しようとする課題】前記ICカードの本人認証に暗証番号を用いる技術によれば、もし暗証番号が盗まれた場合に、ICカードの不正使用を防ぐことができなくなるという問題がある。一方、前記ICカードの本人認証に生体情報を用いる技術によれば、生体情報の照合に必要な処理の処理量が多いこと、決済時毎に生体情報の取得を行わなければならないことなどより、本人認証に必要となる処理時間、利用のコストが大きくなってしまうという問題がある。

【００１１】すなわち、ICカードの本人認証を高い確度で行おうとすると高コストとなり、低コストでICカードの本人認証を行おうとすると本人認証の確度は低くなるという関係が生じる。そして、このようにコストと確度はトレードオフの関係にあるため、どのようなコストをかけてどのような確度で本人認証を行うかは、本人認証によって守るべき価値に応じて最適化するのが合理的であるが、電子マネーやクレジットカードの場合、本人認証によって守られる価値は、個々のICカードの利用状況によって刻々変化するため、前述した暗証番号と生体情報の一方、もしくは、両方を用いることによっては、このような最適化を行うことができない。

【００１２】そこで、本発明は、本人認証に要するコストと本人認証の確度との関係を本人認証によって守るべき価値に応じて動的に最適化することができるICカード決済装置を提供することを課題とする。

6

【００１３】また、前記ICカードの本人認証に暗証番号を用いる技術によれば、ICカードの正当な所有者が暗証番号を忘れてしまった場合には、正当な所有者であっても、ICカードを使用できなくなってしまうという問題がある。そこで、本発明は、正当な所有者であれば、暗証番号を忘れてしまった場合でも、ICカードを利用可能とすることのできるICカード決済装置を提供することを課題とする。

【００１４】また、前記ICカードの本人認証に生体情報を用いる技術によれば、決済時の生体情報の取得、たとえば、指紋の取得に際し、ICカードの所有者に不快感を与えてしまうという問題がある。

【００１５】そこで、本発明は、生体情報の取得に際して、ICカードの所有者に与える不快感を軽減することも課題とする。

【００１６】

【課題を解決するための手段】前記課題達成のために本発明は、たとえば、ICカードの正当な所有者の暗証番号と生体情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置であって、決済を行う金額の入力を受け付ける決済額受け付け手段と、ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、入力された決済を行う金額が所定値より低額である場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第１決済手段と、入力された決済を行う金額が所定値より高額である場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第２決済手段とを有することを特徴とするICカード決済装置を提供する。

【００１７】このようなICカード決済装置によれば、低額の決済時には、暗証番号のみの迅速な本人認証を、高額の決済時には、生体情報を用いた確度の高い本人認証を行うので、本人認証によって守るべき価値の一つ、すなわち、決済がICカードの不正使用である場合の損害額となる決済金額に応じて、動的に本人認証の確度とコストを最適化することができる。

【００１８】また、本発明は、前記課題達成のために、たとえば、ICカードの正当な所有者の暗証番号と生体情報とが記憶されたＩＣカードを用いて、商取引の決済を行うICカード決済装置であって、ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、両暗証番号が一致しない場合に、さらに、前記生体情報読み取り

手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う決済手段とを有することを特徴とするICカード決済装置を提供する。

【００１９】このようなICカード決済装置によれば、通常の決済時は暗証番号を用いた本人認証により迅速に決済を行うことができると共に、暗証番号を知らない、すなわち、疑義あるユーザに対しては、本人認証を生体情報を用いた本人認証により高い確度で行って、決済処理を行うことができるようになる。逆の見方をすれば、正当なユーザは暗証番号をもし忘れても、ICカードによる買い物をすることができるようになる。

【００２０】また、本発明は、前記課題達成のために、ICカードに記憶された当該ICカードの正当な所有者の暗証番号と指紋情報とを用いて、ICカード使用者の認証をおこなうICカード処理装置であって、ICカード使用者より、指先による暗証番号の入力を受け付ける入力部と、当該入力部に暗証番号入力のために置かれた指先から指紋情報を読み取る読み取り部とを有することを特徴とするICカード処理装置を提供する。

【００２１】このようなICカード処理装置によれば、ICカード使用者に指紋情報の読み取りを意識させることなく、ICカード使用者が暗証番号を入力時に指紋情報を読み取ることができる。したがって、指紋読み取り時のICカード使用者の不快感を軽減することができる。

【００２２】

【発明の実施の形態】以下、本発明の一実施形態について説明する。

【００２３】まず、第１の実施形態について説明する。

【００２４】図１に、本実施形態に係るＩＣカード決済端末の構成を示す。

【００２５】本ICカード決済端末は、クレジット決済処理を行うクレジット端末であり、図中、１はクレジット端末、１０はクレジット端末１にリムーバルに装着されるＩＣカードである。また、クレジット端末１中、２はキー入力部、３は表示部、４はレシートの印刷部、５は演算処理部、６はクレジットセンタと接続するためのモデム部、７は取引履歴情報記憶部、８はＩＣカード読み書き部、９は指紋読み取り部である。また、ICカード１０中、１１は接続部、１２は演算処理部、１３は取引履歴情報記憶部、１４はＩＤ情報記憶部、１５は暗証番号記憶部、１６は指紋情報記憶部である。

【００２６】ここで、ＩＤ情報記憶部１４には各ＩＣカード毎に固有のクレジット番号が格納されおり、暗証番号記憶部１５にはユーザーが登録した暗証番号が格納されており、指紋情報記憶部１６にはユーザーが登録した指紋の情報が格納されている。

【００２７】次に、ICカード１０の取引履歴情報記憶部１３には図２に示す取引履歴情報が蓄積される。

【００２８】図示するように取引履歴情報は、買い物した取引日、買い物金額、累積金額、累積回数よりなる。これらは、このICカードによるクレジットによって買い物をすると、その決済を行ったクレジット端末１により格納される。ここで、累積金額は、このICカードによるクレジットによって行った買い物の買い物金額の累積であり、累積の購入回数はこのICカードによるクレジットによって行った買い物の回数である、ただし、後述するように、累積金額と累積回数は、このICカードによるクレジットによって買い物の決済を行うクレジット端末１が、このICカードのクレジット番号をクレジットセンタに照会して、過去の不正使用がないことを確認できた場合に初期化され、次回の買い物では累積回数は１、累積金額は当該次回の買い物金額となる。図の例は、No. ７，４の買い物のときに、その決済を行ったクレジット端末１が、このICカードのクレジット番号をクレジットセンタに照会して、過去の不正使用がないことを確認した場合を示している。

【００２９】以下、本実施形態に係るクレジット端末１の動作について説明する。

【００３０】図３に、クレジット端末１の演算処理部５が行う決済時の動作の手順を示す。

【００３１】図示するように、クレジット端末１の演算処理部５は、ユーザーがＩＣカード１０をクレジット端末１に挿入することにより装着すると（ステップ１０２）、ICカード読み書き部８にＩＣカード１０に電源、クロック、リセット信号を供給させ、ＩＣカードを活性化する。この結果、クレジット端末１０の演算処理部５は、接続部１１、ＩＣカード読み書き部８を介してＩＣカード内の情報を読み出すことが可能となる。

【００３２】次に、店員が買い物金額を入力部２よりクレジット端末に入力すると（ステップ１０３）、演算処理部５は、まず始めに支払いを行うかどうかの確認画面を表示部３に表示させる（ステップ１０４）。そして、ユーザーが支払いを行うことを入力部２より選択した場合は、さらに、入力部２よりユーザからの暗証番号の入力を受け付ける（ステップ１０５）。一方、ユーザーが支払いを行なわいことを入力部２より選択した場合には、ICカード読み書き部８にICカード１０を排出させ（ステップ１１４）、処理を終了する（ステップ１１５）。

【００３３】ステップ１０５で暗証番号が入力されると、演算処理部５は、ICカード１０の演算処理部１２に暗証番号を渡し、入力された暗証番号と、ICカード１０の暗証番号記憶部１５に格納された番号とを比較させ、その結果より両者が一致したかを確認する（ステップ１０６）。そして、一致を確認できなかった場合には、ICカード読み書き部８にICカード１０を排出させ（ステップ１１４）、処理を終了する（ステップ１１５）。

【００３４】一方、ステップ１０６で、暗証番号の一致を確認できた場合には、その後、買い物金額があらかじ

め設定した金額値を超えるかどうかの判定を行う（ステップ１０７）。そして、買い物金額があらかじめ設定した金額値を超えていない場合には、本人認証が成立したものとしてステップ１１１に進む。

【００３５】一方、ステップ１０７で買い物金額が設定値を超えていると判定された場合には、ここでクレジットセンタにオンライン照会を行い、ユーザーの使用するＩＣカードで過去に不正な使用がないかを確認する（ステップ１０８）。この場合、モデム６を介して電話回線によりクレジットセンタとデータのやり取りを行う。そして、過去に不正な使用がないことを確認できなかった場合には、ICカード１０を排出し（ステップ１１４）、処理を終了する（ステップ１１５）。

【００３６】一方、ステップ１０８で、過去に不正な使用がないことを確認できた場合には、指紋読み取り部９によりユーザーの指紋を読み取る（ステップ１０９）。そして、演算処理部５は、ICカード１０の演算処理部１２に読み取った指紋の情報を渡し、これと、ICカード１０の指紋情報記憶部１６に格納された指紋情報とを比較させ、その結果より両者が一致したかを確認する（ステップ１１０）。そして、一致を確認できなかった場合には、ICカード読み書き部８にICカード１０を排出させ（ステップ１１４）、処理を終了する（ステップ１１５）。

【００３７】一方、ステップ１１０で指紋の一致を確認できた場合には、本人認証が成立したものとして、ステップ１１１に進む。

【００３８】本人認証が成立した場合に実行されるステップ１１１では、買い物金額、今日の日付に応じて、ICカードの取引履歴情報記憶部１３の取引履歴情報を更新する。

【００３９】また、クレジット端末側１の取引履歴情報記憶部７も更新する（ステップ１１２）。なお、クレジット端末側１の取引履歴情報記憶部７には、買い物の日付、買い物金額、買い物に使われたICカード１０のクレジット番号などを記憶する。

【００４０】そして、印刷部４によりレシートを発行する（ステップ１１３）と共に、ＩＣカード１０を排出して（ステップ１１４）、処理を終了する（ステップ１１５）。

【００４１】なお、ステップ１１１でのICカードの取引履歴情報記憶部１３の取引履歴情報の更新では、前述したように、累積金額、累積回数も更新する。また、前述したように、累積金額、累積回数はステップ１０８で過去に不正な使用がないことを確認できた場合には、次回の買い物の際に初期化するが、これは、たとえば、ステップ１０８で過去に不正な使用がないことを確認できた場合に、その旨を、取引履歴情報記憶部１３の取引履歴情報の過去に不正な使用がないことを確認した買い物に対応づけて記憶し、ステップ１１１において前回の買い物に対応づけて過去に不正な使用がないことを確認できたことが記憶されている場合には、ステップ１１１のICカードの取引履歴情報記憶部１３の取引履歴情報の更新において、累積金額、累積回数を初期化するようにすればよい。または、ステップ１０８で過去に不正な使用がないことを確認できた場合に、その時の取り引き終了時に、取引履歴情報記憶部１３の取引履歴情報を消去するようにしてもよい。

【００４２】以上、本発明の第１の実施形態について説明した。

【００４３】以上のように、本第１実施形態では、買い物金額が設定値以下の場合は暗証番号により本人認証が行われるが、この場合はオンライン照会は行われないため、短時間で処理を終わらせることができる。一方、買い物金額が設定値を超える場合は、オンライン照会が行われると共にユーザーの指紋により再度本人認証が行われるため、カードと暗証番号を盗まれて悪用された場合にも不正使用を防ぐことができる。すなわち、本第１実施形態によれば、低額な買い物時には、暗証番号のみの迅速な本人認証を、高額な買い物時には、指紋を用いた確度の高い本人認証を行うので、本人認証によって守るべき価値の一つ、すなわち、買い物がICカードの不正使用である場合の損害額となる買い物金額に応じて、動的に本人認証の確度とコストを最適化することができる。

【００４４】なお、指紋情報の確認に関しては、セキュリティの面では安全であるため、以上の説明では、ＩＣカード内の演算処理部１２で比較を行うものとした。しかしながら、処理時間などで問題がある場合は、クレジット端末内の演算処理部５で処理を行うようにすることもできる。

【００４５】以下、本発明の第２の実施形態について説明する。本第２実施形態は、前記第１実施形態における図３の処理を、図４に示すように、買い物金額が設定値を超えた場合のみならず、累積金額が設定値を超えた場合（ステップ２０１）と、累積回数が設定値を超えた場合（ステップ２０２）にも、オンライン照会（ステップ１０８）と、指紋の比較（ステップ１０９、１１０）を行い、その結果、過去の不正無しと指紋の一致が確認できたならば本人認証が成立したとするようにしたものである。

【００４６】本第２実施形態によれば、前記第１実施形態の効果に加え、累積金額が設定値を超えた場合と、累積回数が設定値を超えた場合にも指紋を用いた確度の高い本人認証を行う。ここで、累積金額や累積回数は、そのICカードが不正使用され続けた場合の損害額の大きさに比例するものと推定できるので、本第２実施形態によれば、前記第１実施形態に対し、さらに、本人認証によって守るべき価値の一つである、連続不正使用による損害額の大きさに応じて、動的に本人認証の確度とコストを最適化することができる。

【００４７】なお、以上の第１、第２本実施形態では、買い物金額、累積金額、累積回数に関し、オンライン照合と指紋の一致の確認を行う条件を同じとしたが、これらを異なる条件としてもよい。また、この場合には、累積金額、累積回数は指紋の一致が確認できたときに初期化するようにしてもよい。

【００４８】以上、本発明の第１、第２の実施形態によれば、不正による損害額が小さいと見積もられる場合には暗証番号のみの本人認証となるため、スーパーやコンビニエンスストアなどのようにお客さんの回転が早いお店でもスムーズに処理を行うことができる。一方、不正による損害額が大きくなる可能性があると見積もられる場合には指紋情報による本人認証も行うため、暗証番号が盗まれた場合でも不正使用を防ぐことが可能となり、高額な損害額の発生を防止することができる。また、指紋情報による本人認証と暗証番号による認証も行うため、生体情報による本人認証のみを行う場合に比べ生体情報による本人認証の精度が低くても、本人認証の信頼性はある程度確保できる。このため、生体情報による本人認証のためにICカードに記憶する生体情報の量や、生体情報の比較の処理のための負荷を低減することができる。

【００４９】以下、本発明の第３の実施形態について説明する。

【００５０】本第３実施形態は、前記第１実施形態における図３の処理を、図５に示すように、ステップ１０５で入力された暗証番号が間違っていた場合には、買い物金額が設定値を超えていない場合には（ステップ３０３）、指紋の比較（ステップ３０１、３０２）を行い、指紋が一致した場合には、暗証番号が間違っていても本人認証が成立したものとし、買い物金額が設定値を超えている場合には（ステップ３０３）、指紋の比較（ステップ３０１、３０２）とオンライン照会（ステップ３０４）とを行い、その結果、指紋の一致と過去の不正無しとが確認できたならば暗証番号が間違っていても本人認証が成立したものとする。ただし、暗証番号が間違っていた場合には、買い物金額が設定値を超えていない場合にもオンライン照会を行うようにしてもよい。また、図５の処理は、ユーザの選択に応じてステップ１０５の暗証番号の入力を省略し、常にステップ１０６で暗証番号が間違っていると判定させるようにすることにより、暗証番号の入力を省略したいユーザについては暗証番号の入力を求めないようにするようにしてもよい。

【００５１】また、前記第２実施形態と同様に、累積金額や累積回数が設定値を超えている場合に、買い物金額が設定値を超えている場合と同様の処理を行うようにしてもよい。

【００５２】以上、本第３実施形態によれば、前記第１、第２実施形態に対し、さらに、ユーザが暗証番号を忘れた場合にも、暗証番号を知らない、すなわち、疑義

あるユーザに対して本人認証を指紋を用いた本人認証により高い確度で行って、決済処理を行うことができるようになる。逆の見方をすれば、正当なユーザは暗証番号をもし忘れても、ICカードによる買い物をすることができるようになる。

【００５３】以下、本発明の第４の実施形態について説明する。

【００５４】本第４実施形態は、前記第３実施形態における図５の処理を、図６に示すように、ステップ１０５で入力された暗証番号が間違っていた場合に、指紋の比較（ステップ３０１、３０２）または指紋の比較（ステップ３０１、３０２）とオンライン照会（ステップ３０４）で本人認証が成立したならば、暗証番号の再登録を行うかを表示部３を介してユーザに問い合わせ（ステップ４０１）、暗証番号が入力部２により入力されたならば（ステップ４０２）、ＩＣカード１０の暗証番号記憶部１５の暗証番号を入力された暗証番号に更新する（ステップ４０３）ようにしたものである。

【００５５】なお、この場合は、買い物金額が設定値を超えていない場合にもオンライン照会を行うようにするのがよい。

【００５６】また、前記第２実施形態と同様に、累積金額や累積回数が設定値を超えている場合に、買い物金額が設定値を超えている場合と同様の処理を行うようにしてもよい。

【００５７】以上、本第４実施形態によれば、前記第３実施形態に対し、さらに、指紋を用いた本人認証によって高い確度でユーザを認証し、認証できたユーザに対しては、迅速、簡便な暗証番号の再登録サービスを提供することができるようになる。

【００５８】以下、本発明の第５の実施形態について説明する。

【００５９】図７に示すように、本第５実施形態は、前記第４実施形態における、図６の処理からステップ１０７～１１０、３０３、３０４を省略したものである。

【００６０】すなわち、本第５実施形態では、買い物金額が設定値を超えているかどうかにかかわらず、入力された暗証番号が正しい場合には常に本人認証が成立したものとし、入力された暗証番号が間違っている場合にのみ指紋の比較（ステップ３１５、３１６）を行い、指紋が一致した場合には、暗証番号が間違っていても本人認証が成立したものとする。なお、入力された暗証番号が間違っている場合には、オンライン照会を行うようにしてもよい。

【００６１】これにより通常は暗証番号を用いた迅速な決済処理を行うことができる。また、ユーザが暗証番号を忘れた場合にも、暗証番号を知らない、すなわち、疑義あるユーザに対して本人認証を指紋を用いた本人認証により高い確度で行って、決済処理を行うことができる。逆の見方をすれば、正当なユーザは暗証番号をもし

忘れても、ICカードによる買い物をすることができるようになる。また、指紋を用いた本人認証によって高い確度でユーザを認証し、認証できたユーザに対しては、迅速な暗証番号の再登録サービスを提供することができる。

【００６２】以上、本発明に係るICカード決済端末がクレジット端末である場合の実施形態を、第１～第５の実施形態として説明した。

【００６３】以下、本発明に係るICカード決済端末が、電子マネーの決済を行うPOS端末である場合の実施形態を第６の実施形態として説明する。

【００６４】図８に、本実施形態に係るPOS端末の構成について示す。

【００６５】図中、１７はPOS端末であり、２６は購入者が使用するICカード、７１は販売者が使用するICカードである。

【００６６】また、POS端末中、１８はキー入力部、１９は表示部、２０はレシートの印刷部、２１は演算処理部、２２はモデム部、２３は取引履歴情報記憶部、２４はＩＣカード読み書き部、２５は指紋読み取り部である。また、ICカード２６中、２７は接続部、２８は演算処理部、２９は金額情報記憶部、３０はＩＤ情報記憶部、３１は暗証番号記憶部、３２は指紋情報記憶部である。ここで、金額情報記憶部２９には、電子マネーとして使用可能な金額が記憶されている。なお、ICカード７１の内部構成は、ICカード２６と同様である。

【００６７】このようなPOS端末１７の動作について説明する。

【００６８】図９に、POS端末１７の演算処理部２１が行う決済時の動作の手順を示す。

【００６９】ただし、ここでは、既に販売者のICカード７１がPOS端末１７に装着され、既に販売者のICカード７１についての本人認証は完了しているものとして説明する。

【００７０】図示するように、POS端末１７の演算処理部２１は、購入者がＩＣカード２６をPOS端末１７に挿入することにより装着すると（ステップ５０２）、販売者または購入者より、購入者のICカード２６から販売者のICカード７１に移動する電子マネーの金額である移動金額の入力を入力部１８を介して受け付け（ステップ５０３）、その後、購入者より暗証番号の入力を入力部１８を介して受け付ける（ステップ５０４）。

【００７１】そして、暗証番号が入力されると、演算処理部２１は、ICカード２６の演算処理部２８に暗証番号を渡し、入力された暗証番号と、ICカード２６の暗証番号記憶部３１に格納された番号とを比較させ、その結果より両者が一致したかを確認する（ステップ５０５）。そして、一致を確認できなかった場合には、ステップ５０７に進む。

【００７２】一方、ステップ５０５で暗証番号の一致が確認できた場合には、買い物金額があらかじめ設定した金額値を超えるかどうかの判定を行う（ステップ５０６）。そして、買い物金額があらかじめ設定した金額値を超えていない場合には、本人認証が成立したものとしてステップ５０９に進む。一方、買い物金額があらかじめ設定した金額値を超えている場合には、ステップ５０７に進む。

【００７３】ステップ５０７では、指紋読み取り部２５によりユーザーの指紋を読み取る。そして、演算処理部２１は、ICカード２６の演算処理部２８に読み取った指紋の情報を渡し、これと、ICカード２６の指紋情報記憶部３２に格納された指紋情報とを比較させ、その結果より両者が一致したかを確認する（ステップ５０８）。そして、一致を確認できなかった場合には、ICカード読み書き部２４にICカード２６を排出させ（ステップ５１２）、処理を終了する（ステップ５１３）。

【００７４】一方、ステップ５０８で指紋の一致を確認できた場合には、本人認証が成立したものとして、ステップ５０９に進む。

【００７５】本人認証が成立した場合に行われるステップ５０９では、購入者用のICカード２６の金額情報記憶部２９に記憶されている電子マネーを、入力された移動金額分、販売者用のICカードの金額情報記憶部に移動することにより決済を行う。より具体的には、購入者用のICカード２６の金額情報記憶部２９に記憶されている電子マネーとして使用可能な金額を移動金額分減じ、販売者用のICカード７１の金額情報記憶部に記憶されている電子マネーとして使用可能な金額を移動金額分増加させる。

【００７６】次に、ステップ５１０では、POS端末１７の取引履歴情報記憶部２３に決済の内容を記憶する。たとえば、買い物の日付、買い物金額、買い物に使われたICカード２６のID情報記憶部３０に記憶されているIDなどを記憶する。そして、印刷部２０によりレシートを発行する（ステップ５１１）と共に、ＩＣカード２６を排出して（ステップ５１２）、処理を終了する（ステップ５１３）。

【００７７】以上、本発明の第６実施形態について説明した。

【００７８】なお、以上では購入者用のICカード２６から販売者用のICカード７１に電子マネーを移動する場合について説明したが、本第６実施形態は、たとえば、電話回線を介して銀行からICカード２６に電子マネーを移動する場合にも同様に適用することができる。この場合は、POS端末は、図８のステップ５０９において、モデム２２を介して、銀行から移動金額分の電子マネーを受け取り、これをICカード２６の金額情報記憶部２９に記憶されている電子マネーに加える。

【００７９】また、本第６実施形態は、前記第２実施形態と同様に、累積金額や累積回数を、ICカード２６に記

憶し、これらが設定値を超えている場合に、移動金額が設定値を超えている場合と同様の処理を行うようにしてもよい。また、前記第１、第２実施形態のように、暗証番号が一致しなかった場合には、無条件に本人認証が成立しない者として、決済を行えないようにしてもよい。

【００８０】また、暗証番号が一致しなかった場合にも指紋が一致した場合に本人認証が成立したとする場合には、前記第４実施形態と同様に、指紋の一致するICカードの所有者が、暗証番号の再登録をすることができるようにしたり、暗証番号の入力を省略したいユーザについては暗証番号の入力を求めないようにするようにしてもよい。

【００８１】また、前記第５実施形態のように、買い物金額が設定値を超えているかどうかにかかわらず、入力された暗証番号が正しい場合には常に本人認証が成立したものとし、入力された暗証番号が間違っている場合にのみ指紋の比較を行い、指紋が一致した場合には、暗証番号が間違っていても本人認証が成立したものとするようにしてもよい。

【００８２】以上、本第６実施形態によれば、電子マネーの決済についても、前記クレジット端末に関する各実施形態と同様の効果を達成することができる。

【００８３】さて、近年ではインターネットの普及により、パソコンを使ったインターネットショッピングが広まってきたが、この場合、電子マネーによる決済がセキュリティや手数料などの点でクレジット等に比べると優れている。

【００８４】そこで、以下では、本発明に係るICカード決済端末が、電子マネーを用いたインターネットショッピングを行うパーソナルコンピュータである場合の実施形態を、第７の実施形態として説明する。

【００８５】図１０に、この場合のパーソナルコンピュータの構成を示す。

【００８６】図中、３３はパーソナルコンピュータ、４２はICカードである。また、ICカード４２中、４３は接続部、４４は演算処理部、４５は金額情報記憶部、４６はＩＤ情報記憶部、４７は暗証番号記憶部、４８は指紋情報記憶部、４９は個人情報記憶部である。個人情報記憶部４９にはICカード所有者の生年月日、年令、性別、国籍などの個人情報が記憶されている。また、パーソナルコンピュータ３３中、３４はキー入力部、３５は表示部、３６は印刷部、３７は演算処理部、３８はモデム部、３９はカスタマイズ情報記憶部、４０はＩＣカード読み書き部である。カスタマイズ情報記憶部３９には、個人情報に応じて、どのようにインターネットショッピングのユーザインタフェースをカスタマイズするかが記憶されている。ただし、パーソナルコンピュータ３３中の各部は、パーソナルコンピュータ３３が、所定のソフトウエアを実行することによりパーソナルコンピュータ３３上に実現される機能部である。

【００８７】さて、本実施形態では、インターネットショッピングの利便性を高めるために、ＩＣカード４２内の個人情報記憶部４９にユーザーの個人情報を格納して、これらの情報によりインターネットショッピングに利用する画面の文字サイズ、言語、メニュー内容などを、ICカードの所有者に応じてカスタマイズする。

【００８８】図１１に、パーソナルコンピュータ３３の演算処理部３７が行う処理の手順を示す。

【００８９】まず、ＩＣカードを挿入されると（ステップ６０２）、ICカード４２の個人情報記憶部４９に格納された生年月日、年令、性別、国籍などの個人情報を読み取る（ステップ６０３）。

【００９０】そして、センタと協調してモデム３８を介してセンタからダウンロードされるデータを、読み取った個人情報に応じてカスタマイズし、表示部３５より表示する（ステップ６０４）。カスタマイズする内容としては、ショッピングカタログの内容、文字サイズ、言語などがある。たとえば、若者と高齢者、女性と男性で、利用者に提供するショッピングカタログの内容を異なるものとする。

【００９１】次に、利用者より購入する商品の番号と金額情報の入力を受け付けると（ステップ６０５）、次に利用者がＩＣカード４２の所有者本人であることを確認するために暗証番号の入力を受け付け（ステップ６０６）、暗証番号が一致した場合は、入力された金額分の電子マネーをセンタに移動する決済を行う（ステップ６１０）。また、間違った暗証番号が入力された場合には、指紋読み取り部４１によりユーザーの指紋を読み取り（ステップ６０８）、ＩＣカード４２内の指紋情報記憶部４８に格納された指紋情報と一致するかを確認し（ステップ６０９）、一致した場合は入力された金額分の電子マネーをセンタに移動する決済を行い（ステップ６１０）、取引履歴をパーソナルコンピュータに記憶する（ステップ６１１）。

【００９２】そして、利用者より、買い物の終了が選択された場合（ステップ６１２）、及び、暗証番号も指紋も一致しなかった場合には、ICカード４２を排出し（ステップ６１３）、処理を終了する（ステップ６１４）。買い物を続ける場合は、ステップ６０４よりの処理を行う。

【００９３】以上、本発明の第７実施形態を説明したが、本第７実施形態において、前記第６実施形態と同様に、暗証番号が一致した場合にも、入力された金額が設置値より大きい場合には、さらに指紋の一致を確認し、一致した場合にのみ、ステップ６０８の決済を行うようにしてもよい。また、個人情報が示す年令が子供を示す場合には、アダルト情報にアクセスすることができないようにしてもよい。また、また、個人情報が示す年令が子供を示す場合には、低額の取り引きしか行えないように制限をかけるようにしてもよい。

17

【００９４】なお、本第７実施形態における個人情報に応じたユーザインタフェースのカスタマイズは、クレジット端末、POS端末、電子マネーを取り扱う各種電子マネー端末など、各種装置にも、同様に適用することができる。

【００９５】たとえば、図１２に示すような、暗証番号のみで本人認証を行う、オフラインで動作する電子財布端末にも適用することができる。

【００９６】図１２において、５０は電子財布端末であり、電子財布端末５０中、５１はキー入力部、５２は表示部、５３は演算処理部、５４はカスタマイズ情報記憶部、５５はＩＣカード読み書き部である。また、５６はＩＣカードであり、ICカード５６中、５７は接続部、５８は演算処理部、５９は金額情報記憶部、６０はＩＤ情報記憶部、６１は個人情報記憶部である。

【００９７】電子財布端末５０は、ＩＣカードに格納された残高や取引履歴などの情報を表示するが、このとき、ICカード５６の個人情報記憶部６１から読み出した個人情報により文字サイズ、言語などをカスタマイズする。

【００９８】なお、一般のパソコンのユーザインタフェースのカスタマイズのみをＩＣカードの個人情報により行うようにすることも可能である。例えば、子供や高齢者が操作する場合は、選択できる項目を減らしたり、高機能なアプリケーションは選択できないようにすることにより、あまり迷わずに操作ができるようになる。

【００９９】以下、本発明の第８の実施形態について説明する。

【０１００】本第８実施形態は、以上の各実施形態における指紋の読み取りに関するものである。

【０１０１】さて、指紋情報は警察での犯罪捜査に使われていたことが多いため、ICカードの利用者の指紋情報を読み取る際には生理的に不快感を伴うなどの問題が発生しやすい。そこで、いかに利用者に不快感を与えないように読み取りを行うかが重要である。

【０１０２】そこで、本第８実施形態では、図１３に示すように、暗証番号を入力する数字キーに指紋読み取り部を設けることにより、利用者にはあまり、指紋の読み取りを意識をさせずに指紋を読み取ることができる。通常、暗証番号は４桁以上であるため、数字キーに読み取り部を設けた場合には、暗証番号の桁数と同一回数だけ指紋を読み取ることができる。よって、複数個の読み取りデータを用いて処理を行うことで精度を上げることも可能となる。

【０１０３】一方、暗証番号の入力時には、数字キーによる入力後に必ず入力キー（エンターキー）を押すようにすることにより、図１４に示すように、入力キーのみに指紋読み取り部も設けることも可能である。この場合は、読み取り部は１個になるため、装置のコストを下げることができる。

18

【０１０４】なお、ユーザーの指紋情報は、例えば右手の人差し指から読み取るように統一させることも必要だが、例えば画面の右側にキーを配置して、さらにキーに指の形状の窪みを設けることでユーザーに意識をさせなくても、ある程度は所望の指から指紋を取ることができるようになる。

【０１０５】いずれの場合も、指紋を読み取れなかった場合には、画面にメッセージを出して利用者に説明を行い、再度キーに指を載せて指紋を取得するようにしてもよい。

【０１０６】以上、本発明の実施形態について説明した。

【０１０７】なお、以上の第１実施形態から第７実施形態では、本人認証に用いる生体情報として指紋を用いる場合について説明したが、生体情報としては、掌紋、虹彩、網膜など、その他の生体情報を用いるようにしてもよい。

【０１０８】また、以上の第１実施形態から第６実施形態において、前記第７実施形態と同様にICカードにICカードの所有者の個人情報を記憶し、ICカードに記憶した個人情報を、生体情報の代わりに、もしくは、生体情報と共に用いて本人認証を行うようにしてもよい。たとえば、ICカード利用者から、誕生日や電話番号の入力を受け付け、これと、ICカードに個人情報として記憶された誕生日や電話番号とを比較し、両者が一致した場合に個人情報による本人認証が成立したとするようにする。

【０１０９】

【発明の効果】以上のように、本発明によれば、本人認証に要するコストと本人認証の確度との関係を本人認証によって守るべき価値に応じて動的に最適化することができるICカード決済装置を提供することができる。

【０１１０】また、正当な所有者であれば、暗証番号を忘れてしまった場合でも、ICカードを利用可能とすることのできるICカード決済装置を提供することができる。

【０１１１】また、生体情報の取得に際して、ICカードの所有者に与える不快感を軽減することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係るICカード決済端末の構成を示すブロック図である。

【図２】本発明の第１実施形態に係るICカードに記録する取引履歴情報を示す図である。

【図３】本発明の第１実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図４】本発明の第２実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図５】本発明の第３実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図６】本発明の第４実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図７】本発明の第５実施形態に係るICカード決済端末

の動作を示すフローチャートである。

【図８】本発明の第６実施形態に係るICカード決済端末の構成を示すブロック図である。

【図９】本発明の第６実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図１０】本発明の第７実施形態に係るICカード決済端末の構成を示すブロック図である。

【図１１】本発明の第７実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図１２】本発明の第７実施形態に係るICカード決済端末の他の構成を示すブロック図である。

【図１３】本発明の実施形態に係るICカード決済端末の指紋読み取り部を示す図である。

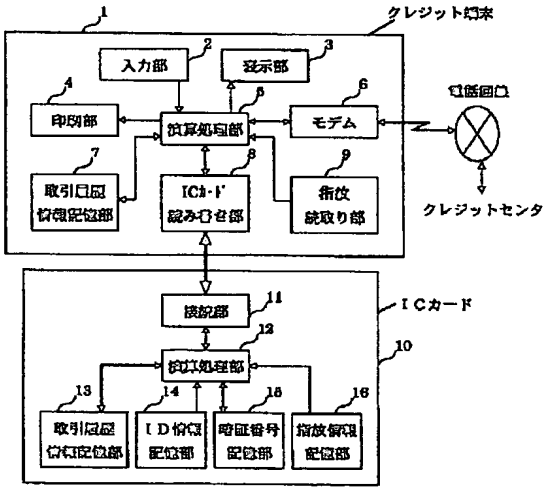
【図１４】本発明の実施形態に係るICカード決済端末の指紋読み取り部を示す図である。

【符号の説明】

１…クレジット端末、２…入力部、３…表示部、４…印刷部、５…演算処理部、６…モデム部、７…取引履歴情報記憶部、８…ＩＣカード読み書き部、９…指紋読み取り部、１０…ＩＣカード、１１…接続部、１２…演算処理部、１３…取引履歴情報記憶部、１４…ＩＤ情報記憶部、１５…暗証番号記憶部、１６…指紋情報記憶部、１７…ＰＯＳ端末、１８…入力部、１９…表示部、２０…印刷部、２１…演算処理部、２２…モデム部、２３…取引履歴情報記憶部、２４…ＩＣカード読み書き部、２５…指紋読み取り部、２６…ＩＣカード、２７…接続部、２８…演算処理部、２９…金額情報記憶部、３０…ＩＤ情報記憶部、３１…暗証番号記憶部、３２…指紋情報記憶部、３３…パーソナルコンピュータ、３４…入力部、３５…表示部、３６…印刷部、３７…演算処理部、３８…モデム部、３９…カスタマイズ情報記憶部、４０…ＩＣカード読み書き部、４１…指紋読み取り部、４２…ＩＣカード、４３…接続部、４４…演算処理部、４５…金額情報記憶部、４６…ＩＤ情報記憶部、４７…暗証番号記憶部、４８…指紋情報記憶部、４９…個人情報記憶部、５０…電子財布端末、５１…入力部、５２…表示部、５３…演算処理部、５４…カスタマイズ情報記憶部、５５…ＩＣカード読み書き部、５６…ＩＣカード、５７…接続部、５８…演算処理部、５９…金額情報記憶部、６０…ＩＤ情報記憶部、６１…個人情報記憶部、７１…ＩＣカード

【図１】

図1



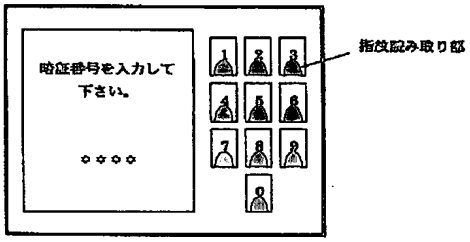
【図２】

図2

No.	取引日	買い物金額	累積金額	累積回数
1	98.9.15	8,000 円	19,800 円	3
2	98.9.13	4,000 円	11,800 円	2
3	98.9.12	7,800 円	7,800 円	1
4	98.9.10	22,000 円	51,900 円	3
5	98.9.5	14,600 円	29,900 円	2
6	98.9.4	15,300 円	15,300 円	1
7	98.9.2	7,500 円	22,000 円	5
8	98.8.30	2,000 円	14,500 円	4
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

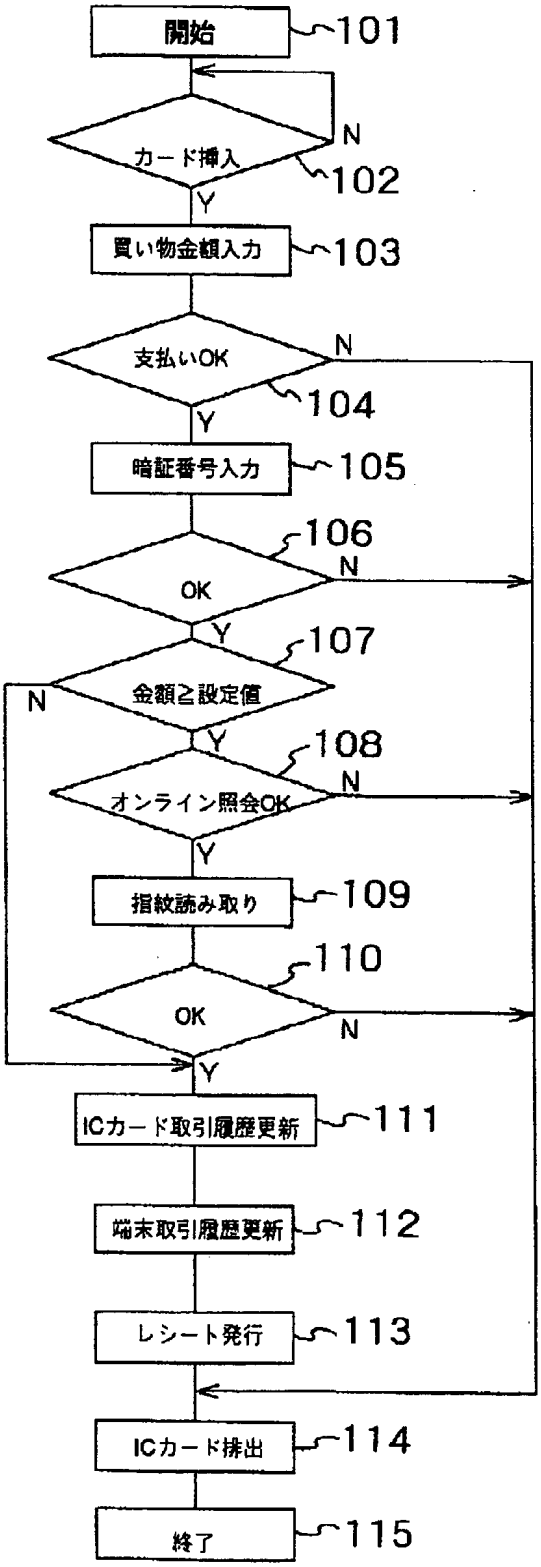
【図１３】

図13



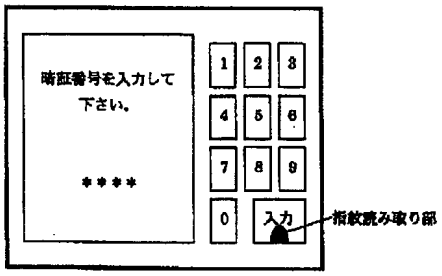
【図３】

図3


開始
101
カード挿入
N
102
Y
買い物金額入力
103
支払いOK
N
104
Y
暗証番号入力
105
106
OK
N
Y
107
金額≧設定値
N
Y
108
オンライン照会OK
N
Y
指紋読み取り
109
110
OK
N
Y
ICカード取引履歴更新
111
端末取引履歴更新
112
レシート発行
113
ICカード排出
114
終了
115

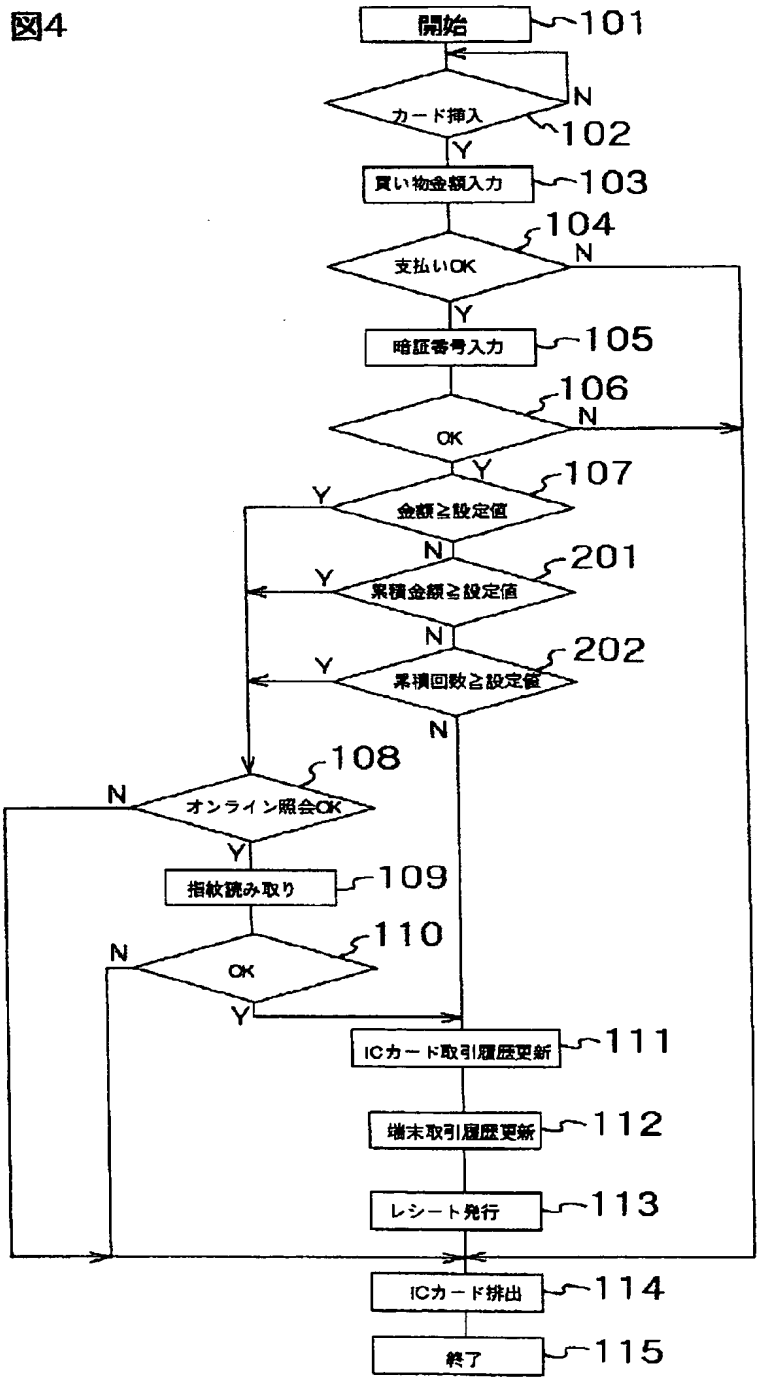
【図１４】

図14


暗証番号を入力して
下さい。
****
1
2
3
4
5
6
7
8
9
0
入力
指紋読み取り部

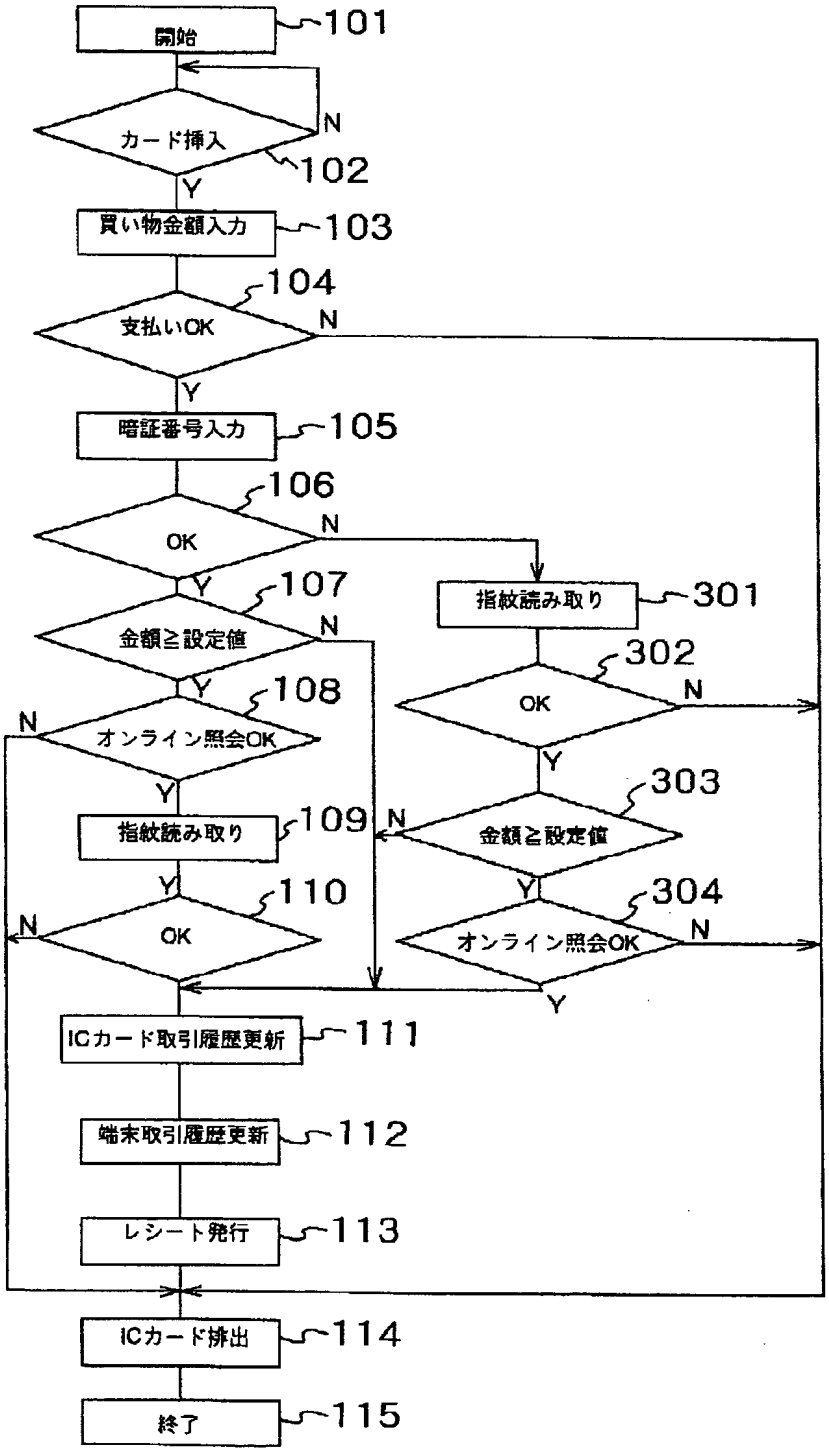
【図４】

図4


開始
101
カード挿入
102
N
Y
買い物金額入力
103
支払いOK
104
N
Y
暗証番号入力
105
OK
106
N
Y
金額≧設定値
107
Y
N
累積金額≧設定値
201
Y
N
累積回数≧設定値
202
Y
N
オンライン照会OK
108
N
Y
指紋読み取り
109
OK
110
N
Y
ICカード取引履歴更新
111
端末取引履歴更新
112
レシート発行
113
ICカード排出
114
終了
115

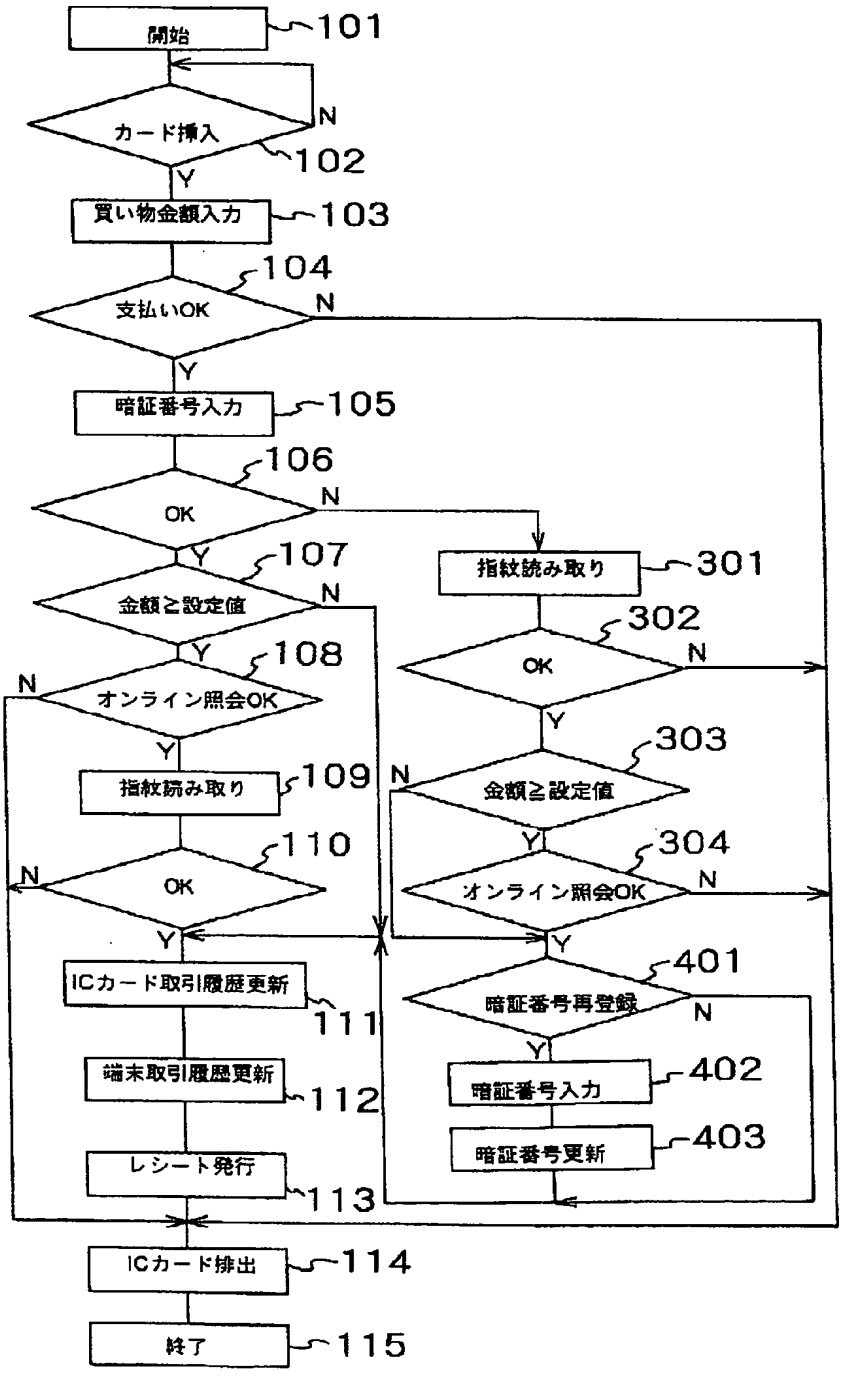
【図５】

図5


開始
101
カード挿入
102
N
Y
買い物金額入力
103
104
支払いOK
N
Y
暗証番号入力
105
106
OK
N
Y
107
金額≧設定値
N
Y
108
オンライン照会OK
N
Y
指紋読み取り
109
Y
110
OK
N
指紋読み取り
301
302
OK
N
Y
303
金額≧設定値
N
Y
304
オンライン照会OK
N
Y
ICカード取引履歴更新
111
端末取引履歴更新
112
レシート発行
113
ICカード排出
114
終了
115

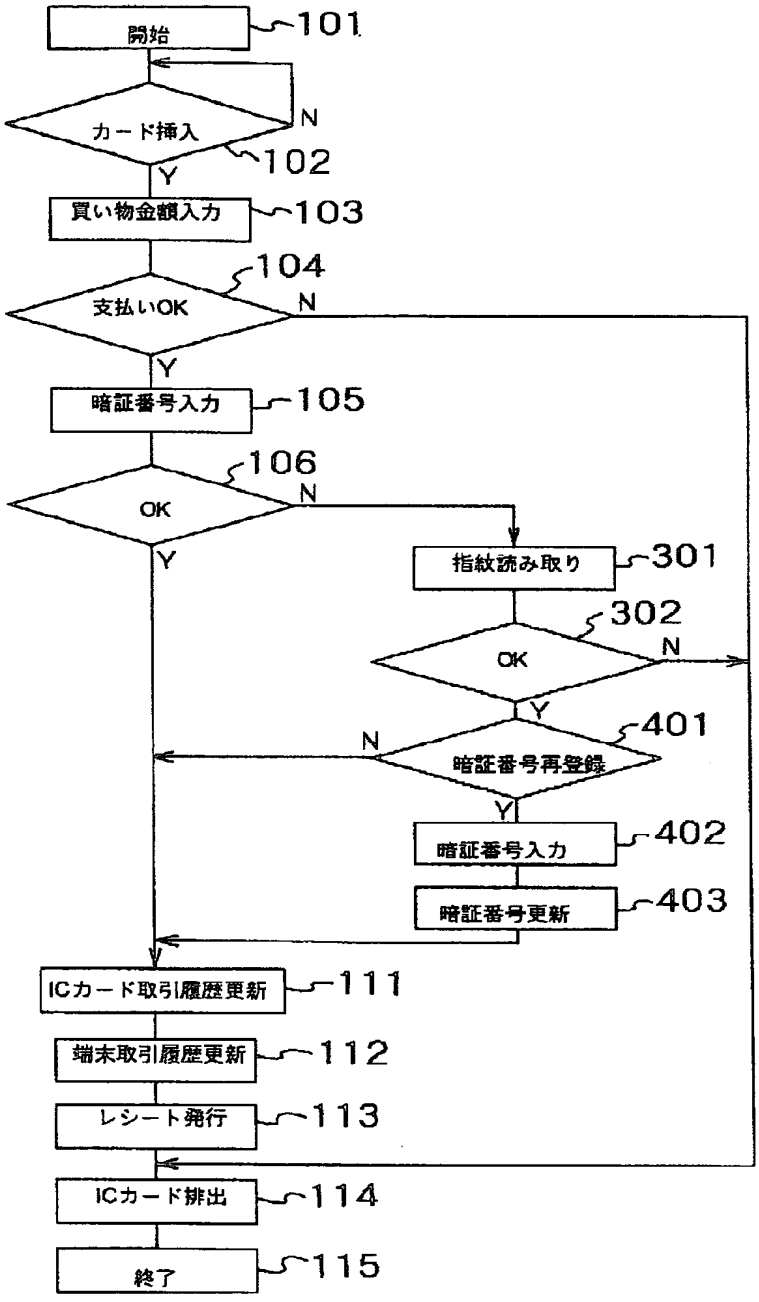
【図６】

図6


開始
101
カード挿入
102
N
Y
買い物金額入力
103
104
支払いOK
N
Y
暗証番号入力
105
106
OK
N
Y
107
金額≧設定値
N
Y
108
オンライン照会OK
N
Y
指紋読み取り
109
110
OK
N
Y
ICカード取引履歴更新
111
端末取引履歴更新
112
レシート発行
113
ICカード排出
114
終了
115
指紋読み取り
301
302
OK
N
Y
303
金額≧設定値
N
Y
304
オンライン照会OK
N
Y
401
暗証番号再登録
N
Y
暗証番号入力
402
暗証番号更新
403

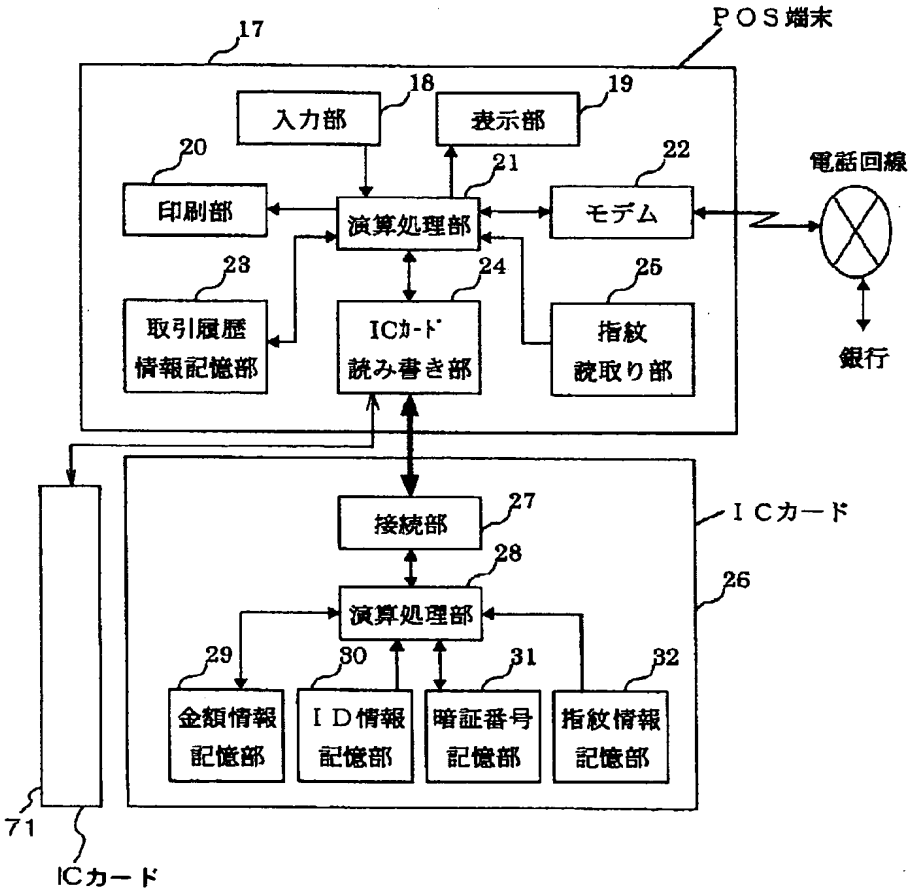
【図７】

図7


開始
101
カード挿入
N
102
Y
買い物金額入力
103
104
支払いOK
N
Y
暗証番号入力
105
106
OK
N
Y
指紋読み取り
301
302
OK
N
Y
401
暗証番号再登録
N
Y
暗証番号入力
402
暗証番号更新
403
ICカード取引履歴更新
111
端末取引履歴更新
112
レシート発行
113
ICカード排出
114
終了
115

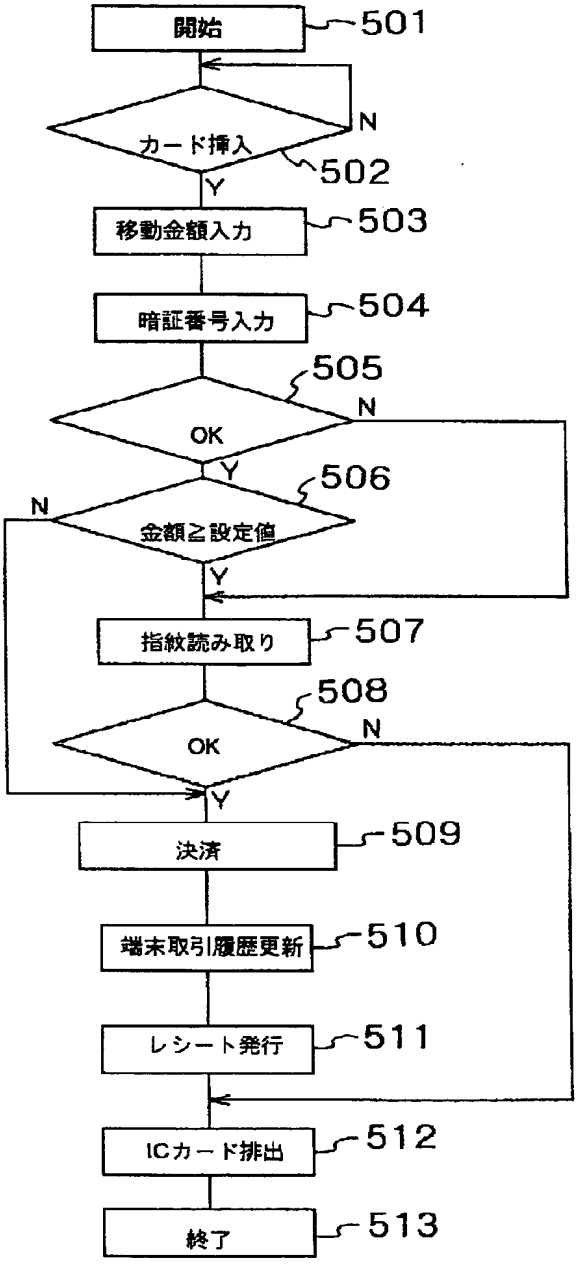
【図８】

図8


17
POS端末
入力部
18
表示部
19
20
印刷部
21
演算処理部
22
モデム
電話回線
28
取引履歴
情報記憶部
24
ICカード
読み書き部
25
指紋
読取り部
銀行
接続部
27
ＩＣカード
28
演算処理部
26
29
金額情報
記憶部
30
ＩＤ情報
記憶部
31
暗証番号
記憶部
32
指紋情報
記憶部
71
ICカード

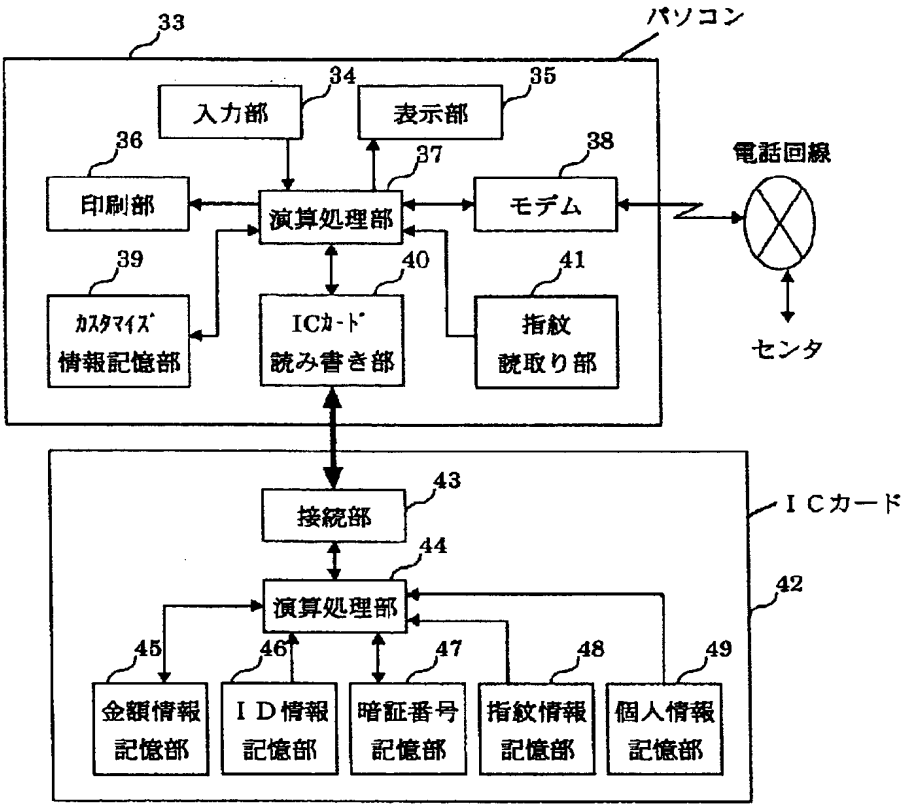
【図９】

図9


開始
501
カード挿入
502
N
Y
移動金額入力
503
暗証番号入力
504
505
OK
N
Y
506
金額≧設定値
N
Y
指紋読み取り
507
508
OK
N
Y
決済
509
端末取引履歴更新
510
レシート発行
511
ICカード排出
512
終了
513

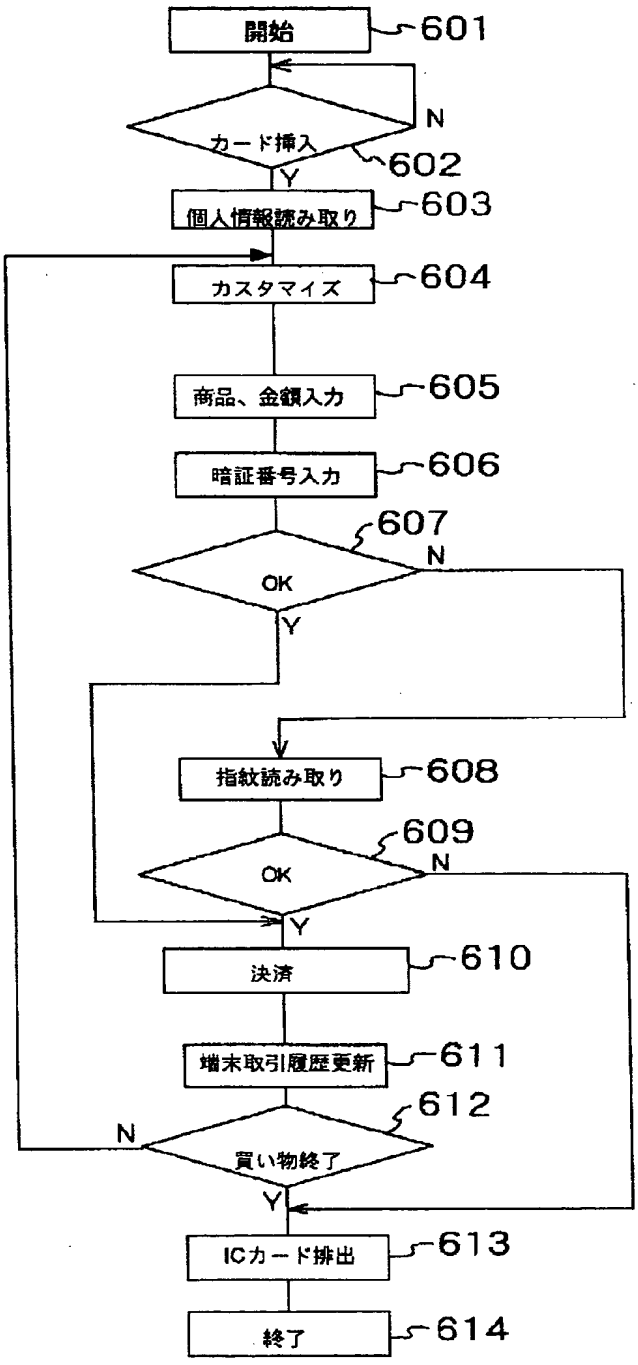
【図１０】

図10


33
パソコン
34
入力部
35
表示部
36
印刷部
37
演算処理部
38
モデム
電話回線
39
ｶｽﾀﾏｲｽﾞ
情報記憶部
40
ICｶｰﾄﾞ
読み書き部
41
指紋
読取り部
センタ
43
接続部
ＩＣカード
44
演算処理部
42
45
46
47
48
49
金額情報
記憶部
ＩＤ情報
記憶部
暗証番号
記憶部
指紋情報
記憶部
個人情報
記憶部

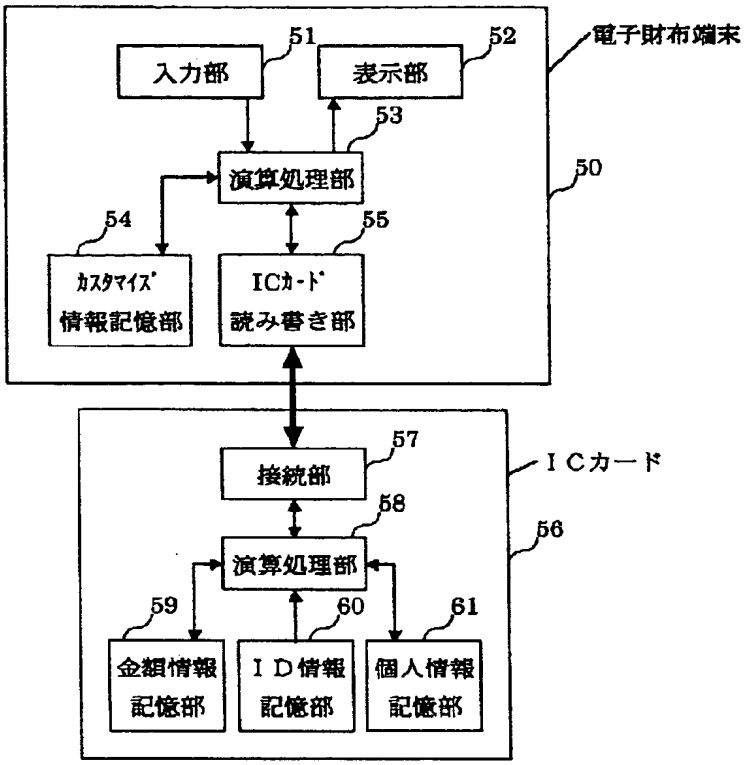
【図１１】

図11


開始
601
カード挿入
602
N
Y
個人情報読み取り
603
カスタマイズ
604
商品、金額入力
605
暗証番号入力
606
607
OK
N
Y
指紋読み取り
608
609
OK
N
Y
決済
610
端末取引履歴更新
611
612
N
買い物終了
Y
ICカード排出
613
終了
614

【図１２】

図12



フロントページの続き

(51) Int. Cl.[7]		識別記号	ＦＩ		テーマコード(参考)
Ｇ０７Ｄ	9/00	４６１	Ｇ０７Ｄ	9/00	４６１Ｂ
Ｇ０７Ｆ	7/12		Ｇ０７Ｆ	7/08	Ｂ
	7/08				Ｒ
					Ｚ

(72)発明者　伊藤　滋行
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　高見　穣
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　井上　雅之
神奈川県横浜市戸塚区吉田町292番地　株式会社日立画像情報システム内
(72)発明者　米田　幸一
神奈川県横浜市戸塚区吉田町292番地　株式会社日立画像情報システム内
(72)発明者　稲光　哲治
神奈川県横浜市戸塚区吉田町292番地　株式会社日立画像情報システム内
(72)発明者　山内　司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内

(72)発明者　井上　喜勇
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内

Ｆターム(参考)　3E040 AA03 DA02 FK09
3E044 AA20 BA05 CA06 DA01 DA05 DA06 DB02 DB05 DC05 DC06 DD02 DE05
5B058 CA27 KA33 KA38 KA40 YA02